WEB APPLICATION FIREWALL

FortiWeb Release Notes

VERSION 5.9.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 20, 2018

FortiWeb 5.9.0 Release Notes

1st Edition

Change log

03/20/2018	Initial release.

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 5.9.0, build 1609.

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day threats. The Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe from:

- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malicious sources
- DoS attacks

For additional documentation, please visit the FortiWeb documentation:

http://docs.fortinet.com/fortiweb/

What's new

Disk partitioning requirement

To support the latest features and enhancements, your FortiWeb needs to be re-partitioned when you upgrade from any version prior to FortiWeb 5.5.

For instructions, see "Repartitioning the hard disk" on page 15.

New and enhanced features

FTP Security

FortiWeb can monitor FTP traffic. You can configure FTP server policies and server pools, and create an FTP security profile that contains rules to enforce these features:

- SSL offloading
- File checks, including antivirus scanning and sending files to FortiSandbox
- FTP command restrictions
- Trusted IP lists
- Geo IP rules
- IP reputation intelligence

FTP Security features are available only in Reverse Proxy mode.

Source NAT (SNAT)

You can configure SNAT policies that translate a matching source IP address to a single IP address or an IP address in an address pool.

Password policy

You can configure a password policy for administrator accounts that set rules for password characteristics, including:

- Minimum length
- Character requirements
- Password reuse limits
- Password expiration intervals

European Union Trusted Service List (TSL) support

You can import TSLs, lists of qualified trust service providers and services, as certificate authorities (CAs) in certificate verification rules and Server Name Indication (SNI) configurations. Import a TSL by either:

- Uploading an XML file of the TSL, or
- Entering the distribution URL of the TSL.

Add TSLs to a CA Group so that FortiWeb can verify X.509 certificates that the qualified service providers use to verify trusted services.

Monitor blocked users

Easily view a list of blocked users. You can sort blocked users according to site publish policies, user tracking rules, and server policies that blocked each user.

NTLM Authentication Delegation

FortiWeb supports NTLM authentication in site publish rules for web applications that use NTLM authentication for single sign-on (SSO) authentication.

Brotli compression

File Compress Policies support Brotli compression.

Server load balancing (SLB) persistence synchronization in High Availability (HA) configurations

When FortiWeb is operating in HA Active-Passive (AP) mode, you can enable **Layer 7 Persistence Synchronization**. This option enables session synchronization when there's a failover that causes the slave appliance to take over as the new master, and is useful for web applications that require sticky sessions.

HA web UI improvements

The High Availability Configuration page has been redesigned to provide you with the ability to modify more commonly used options and features. All functionality remains the same in the CLI.

SNI forwarding

You can configure FortiWeb to forward the hostname of the server that the client is attempting to connect to during the SSL handshake so that the server handles client certificate verification.

HTTP content routing by HTTPS SNI

In a Content Routing Policy, for the **Match Object** option, you can select `HTTPS SNI` so that FortiWeb will forward requests based on the SNI in the SSL handshake.

HTTP content routing reverse matches

In a Content Routing Policy, there is a new option: **Reverse**. When enabled, FortiWeb will route requests to the server pool that do not match the specified values for the **Match Object**.

HTTP/2 for content routing

You can configure FortiWeb to negotiate HTTP/2 with clients during the SSL handshake when the **Deployment Mode** is `HTTP Content Routing`. The corresponding server pool in an HTTP content routing policy should still use HTTP.

HTTP header security enhancement

In a Secure Header Rule, there is a new **Secure Header Type** value: `Content-Security-Policy`. You can configure FortiWeb to insert the Content-Security-Policy (CSP) HTTP header in responses to prevent certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Health Check support for HTTP/2

FortiWeb can perform server health checks via HTTP/2. Health checks allow FortiWeb to determine the status of a server before forwarding traffic.

Health Check enhancement

In a Health Check Rule, for the **Type** option, `HTTP` and `HTTPS` have been merged into `HTTP`. The health check will detect the appropriate protocol for the server when sending the request.

In addition, if you want to test the availability of a specific host, do so in a server pool rule via the **Health Check Domain Name** option.

Response action improvement

A new **Action** for rules and policies is available: `Deny (no log)`. Use this option to deny or block a request that violated a rule or policy without generating a log message.

Severity Level improvement

A new **Severity Level** for rules and policies is available: `Informative`. Use this option for attacks that violated a rule or policy but do not pose a security threat. By default, log messages with a **Severity Level** of `Informative` are hidden in logs; you can adjust the filter settings to display the log messages.

Debug logging improvement

The Console Log has been renamed to the Debug Log, and includes netstat log and core dump log files. You can also upload the symbol table file for use with GDB. Only the `admin` administrator account can download the Debug Log.

Attack and Traffic log improvement

Attack and Traffic logs provide the following information about each log message:

- TLS/SSL version
- Cipher suite

Aggregated attack log field name update

The `Type` field name for some types of aggregated attacks has been modified so that descriptions are more consistent.

Filter Types in custom rules

Improvements have been made to two filter types in custom rules:

1. When the **Filter Type** is `HTTP Header`, you can enable **HTTP Method Check**.
2. When the **Filter Type** is `Source IP`, you can set a reverse match condition.

Data Types for Predefined Patterns

Two new data types for predefined patterns are available:

- Aadhaar Card
- PAN Card

Include predefined data types in a group so that you can use them in an auto-learning profile.

Signature Policy configuration improvements

The **Credit Card Detection** and **Credit Card Detection Threshold** options have been renamed to the **Personally Identifiable Information** and **Detection Threshold** options, respectively. The **Personally Identifiable Information** option includes signatures for the following information:

- Aadhaar Card
- PAN Card
- Canadian Social Insurance Number
- U.S. Social Security Number
- Credit Card

Signature dictionaries improvement

The names of some subclasses for the **Known Exploits** dictionary have been updated.

Target in custom signatures

Custom signature rules contain the `HTTP_METHOD` target. The target(s) in a custom signature describe(s) which part of a request FortiWeb scans for a signature match.

Updating the FDS Proxy

You can poll updates on demand and schedule regular poll updates for the FDS Proxy. It's also easier to view the FDS Proxy status.

Query interval for FortiSandbox malware packages

The interval for querying the FortiSandbox malware signature database was reduced from 10 minutes to one minute.

Timeout interval for holding sessions sent to FortiSandbox

In a File Security Policy, if you enable **Hold Session while Scanning File**, FortiWeb will hold the session for up to 30 minutes while FortiSandbox is scanning the file.

Optional SSL verification

There is a new option for Certificate Verify policies: **Strictly Require Client Certificate**. When enabled, FortiWeb won't accept the SSL handshake from a client if the client can't provide a client certificate for verification. When disabled, FortiWeb will accept the SSL handshake from a client even if the client can't provide a client certificate for verification.

SSL/TLS session ID and ticket reuse

Server pool rules support SSL/TLS session ID and/or ticket reuse. Subsequent requests can reuse active SSL session IDs and tickets to reduce the handshake cost of handling requests.

This feature is available only in Reverse Proxy and True Transparent Proxy modes. For details, see "Creating a server pool" on page 1.

SSL session and ticket timeout interval

When FortiWeb is configured as an SSL server, you can set SSL session and ticket timeout intervals via the CLI. This is available only in Reverse Proxy and True Transparent Proxy modes.

CLI improvements for `diagnose` command

The `diagnose` command has been modified in the CLI. The `hardware` subcommand and options have been updated:

- When you enter the command `diagnose hardware nic list <port_name>`, FortiWeb now displays `speed` and `duplex` information about the specified port.
- When you enter the command `diagnose hardware check`, you no longer have to specify the type of hardware option, and instead enter `sslcard`.

US-only FortiGuard services updates

You can configure FortiWeb to receive FortiGuard services updates from servers located only in the United States.

DHCP enhancement for FortiWeb AWS and Azure

IP address and gateway configurations have been modified in the CLI.

Configuration backup file improvement

When you export backup configuration files, the encryption and compression methods now use the `.zip` file format. This means that you can extract compressed files that are encrypted.

Feature Visibility

Enable or disable the ability to view configuration options for the following features in the web UI:

- FTP Security
- Device Tracking

Azure On-Demand

FortiWeb 5.9.0 offers support for Azure On-Demand.

HA support for FortiWeb AWS and Azure

The following platforms now support HA AA and AP configurations:

- FortiWeb AWS
- FortiWeb AWS On Demand

- FortiWeb Azure
- FortiWeb Azure On Demand

KVM graceful reboot and shutdown

You can gracefully reboot and shutdown FortiWeb-VM running on the KVM platform.

Change and performance notices

HTTP content routing is partially supported when HTTP/2 is enabled

When FortiWeb is deployed in Reverse Proxy mode and HTTP/2 is enabled, HTTP content routing is partially supported. FortiWeb can communicate with clients via HTTP/2, but FortiWeb should communicate with the server or server pool via HTTP. For example, if the **Deployment Mode** is `HTTP Content Routing` and **HTTP/2** is enabled, FortiWeb will negotiate HTTP/2 with clients during the SSL handshake, but the corresponding server pool in an HTTP content routing policy should still use HTTP.

HTTP content routing policies that match X.509 certificate content

In 5.5 Patch 4, the HTTP content routing policy settings that match X.509 certificate content were enhanced to allow you to match values found in either the client certificate's subject field or the extension field. When you upgrade from an earlier release, the upgrade process deletes any HTTP content routing policies that match X.509 certificate content. You can re-create these policies using the enhanced settings.

Log feature after upgrade

The logging feature does not work after you downgrade your FortiWeb 5.5 or later appliance to an earlier version and then upgrade back to the original version.

Software support for FortiWeb 400B and 1000B

FortiWeb 5.4 and later software is not supported on the 400B and 1000B platforms. Fortinet will continue to provide bug fixes to these models with 5.3.X patch releases.

Traffic logs

Very frequent disk writing may cause abnormal disk wear and tear and performance decreases. Fortinet recommends enabling traffic logs only when debugging problems. Disable traffic logs once FortiWeb is operating normally.

Failure to disable traffic logging during normal use may cause premature hard disk failure.

Time required to display data analytics reports

Depending on how much data must be analyzed for a query, data analytics queries can take some time. You should try filtering queries to include data from short periods of time.

Data analytics data set limitations

Due to the large amount of data that can be stored in the data analytics database, data analytics queries can search only up to 1,000,000 records at a time. This will be enhanced in later versions of FortiWeb.

Rebuilding the log aggregation database

In some cases, if the log aggregation database is damaged, the web UI does not display logs correctly on the **Aggregated Attacks** page. For example, duplicate logs may be displayed, or logs may be missing.

To correct these problems, use the following command to rebuild the database:

```
execute db rebuild
```

This operation does not delete any logs. For details, see the *FortiWeb CLI Reference*:

http://docs.fortinet.com/fortiweb/reference

Upgrade instructions

Hardware & VM support

FortiWeb 5.9.0 supports:

- FortiWeb 100D
- FortiWeb 400C
- FortiWeb 400D
- FortiWeb 600D
- FortiWeb 1000D
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000C/3000CFsx
- FortiWeb 3000D/3000DFsx
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000C
- FortiWeb 4000D
- FortiWeb 4000E
- FortiWeb-VM

Repartitioning the hard disk

To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb operating system's disk.

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see "To use the special firmware image to repartition the operating system's disk " on page 16.

For the following FortiWeb-VM tools, you cannot install the special firmware image to repartition the hard disk:

- Citrix XenServer
- Open-source Xen Project
- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See "To repartition the operating system's disk without the special firmware image" on page 16.

Repartitioning affects the operating system's disk (USB/flash disk), not the hard disk. Existing data such as reports and event, traffic, and attack logs, which are on the hard disk, are not affected.

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

To use the special firmware image to repartition the operating system's disk

1. Perform a complete backup of your FortiWeb configuration.

   Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Go to the Fortinet Customer Service & Support website to download the special repartitioning firmware image from the FTP site:

   https://support.fortinet.com/

   Ensure that you download the correct image for your FortiWeb platform.

3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:

   - In the Web UI, go to **System > Status > Status**. Locate the **System Information** widget. Beside **Firmware Version**, click **[Update]**.
   - In the Web UI, go to **System > Maintenance > Backup & Restore**. Select the **Restore** option in **System Configuration**.
   - In the CLI, enter the `execute restore config` command.

   FortiWeb backs up the current configuration, resizes the hard drive partitions, and boots the system.

4. Continue with the instructions in "Upgrading from previous releases" on page 18.

To repartition the operating system's disk without the special firmware image

1. Perform a complete backup of your FortiWeb configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides

2. Use the instructions for your hypervisor platform to detach the log disk from the VM:

   - "To detach the log disk from a Citrix XenServer VM" on page 17
   - "To detach the log disk from a Microsoft Hyper-V VM" on page 17
   - "To detach the log disk from a KVM VM" on page 17

3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.

4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:

- "To attach the log disk to a Citrix XenServer VM" on page 17
- "To attach the log disk to a Microsoft Hyper-V VM" on page 17
- "To attach the log disk to a KVM VM" on page 18

5. Restore the configuration you backed up earlier to the new VM.
6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.
3. For **Description**, enter a new description, and then click **OK**.
4. Select **Hard disk 2** again, and then click **Detach**.
5. Click **Yes** to confirm the detach task.

To detach the log disk from a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the FortiWeb-VM in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (data.vhd)**, and then click **Remove**.
3. Click **Apply**.

To detach the log disk from a KVM VM

1. In Virtual Machine Manager, double-click the FortiWeb-VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.

To attach the log disk to a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the new, FortiWeb 5.5 or later VM, on the Storage tab, select **Hard disk 2**, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. On the Storage tab, click **Attach Disk**.
5. Navigate to the hard disk you detached from the old VM to attach it.
6. Start your new virtual machine.

To attach the log disk to a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the new, FortiWeb 5.5 or later virtual machine in the list of machines, and then, under Actions, click **Settings**.
2. Select **Hard Drive (log.vhd)**, and then click **Browse**.

3. Browse to the hard drive you detached from the old virtual machine to select it.
4. Click **Apply**.
5. Start the new virtual machine.

To attach the log disk to a KVM VM

For KVM deployments, you remove an existing virtual disk from the new VM before you attach the disk detached from the original VM.

1. In Virtual Machine Manager, double-click the new, FortiWeb 5.5 or later VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.
4. Click **Add Hardware**.
5. Click **Storage**, select **Select managed or other existing storage**, and then click **Browse**.
6. Click **Browse Local**.
7. Navigate to the log disk file for the original machine to select it, and then click **Open**.
8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

To download the Customer Service & Support image checksum tool

After logging in to the website, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. This button appears only if one or more of your devices has a current support contract. In the **File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from previous releases

- To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 15.

- If you upgrade from a version of FortiWeb previous to 5.5.4, the upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If you upgrade from a version of FortiWeb previous to 5.3.6, the upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.
- If you upgrade from a version of FortiWeb previous to 5.3.4 and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.

Note: To upgrade from 4.0 MR4, Patch x or earlier, please contact Fortinet Technical Support.

To upgrade from FortiWeb 5.5.x

Upgrade to FortiWeb 5.9.0 directly.

To upgrade from FortiWeb 5.4.x or FortiWeb 5.3.x

Upgrade to FortiWeb 5.9.0 directly after completing the hard disk repartitioning process.

If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see "FortiWeb-VM license validation after upgrade from pre-5.4 version" on page 20.

To upgrade from a version previous to FortiWeb 5.3

FWB5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.

   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:

   https://support.fortinet.com

   In the menus at the top of the page, click **Download**, and then click **Firmware Images**.
4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:

   `/FortiWeb/v5.00/5.3/Upgrade_script/`
5. Download the .zip compressed archive (for example, `FWB5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.

   For example, in the directory where the file `FWB5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

```
FWB5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
```

The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.

7. Resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 15.
8. Upgrade to FortiWeb 5.9.0.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).

   If you upgrade from a previous version of FortiWeb and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.

Upgrading an HA cluster

If the HA cluster is running FortiWeb 4.0 MR4 or later, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it automatically upgrades any standby appliance(s), too; no manual intervention is required to upgrade the other appliance(s). This includes upgrading using the special hard disk repartitioning firmware image for upgrading to 5.5 or later from earlier releases.

If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, contact Fortinet Technical Support for assistance.

Downgrading to a previous release

When you downgrade your FortiWeb 5.9.0 to version 5.1 or 5.0, the basic configuration for your appliance's connections to the network (e.g., IP address and route configuration) is preserved.

FortiWeb-VM license validation after upgrade from pre-5.4 version

On some virtual machine deployments, upgrading FortiWeb-VM from a version previous to 5.4 changes the virtual machine's universal unique identifier (UUID). Because of this change, the first time you upload your existing FortiWeb-VM license, the FortiGuard Distribution Network (FDN) server reports that it is invalid.

To solve this problem, after you have uploaded the license, wait 90 minutes, and then upload the license again.

This issue does not affect FortiWeb-VM deployed on a VMware vSphere hypervisor.

Resolved issues

This section lists issues that have been fixed in version 5.9.0. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
412449	Admin login attempts may prompt for admin authentication credentials from an untrusted host even when all admin accounts have trusted hosts configured.
453666	Trusted IPs may not correctly bypass a malformed HTTP request check in an HTTP Protocol Constraints policy.
461530	Proxyd may crash when FortiWeb performs client certificate verification.
464331	FortiWeb continues sending LDAP queries after a user has been locked out for exceeding the maximum number of login attempts.
466361	If there is a timezone conflict, FortiWeb may have an issue downloading traffic logs for a time period that you specify.
466384	When a request fails, FortiWeb incorrectly sends a TCP RST packet to the client.
466844	If the HTTP header is `Content-type: multipart/related`, FortiWeb may not forward the whole package from the server to the client.
468904	When filtering a signature search by CVE identifier, you cannot enter more than four digits.
468909	PHP Easter Egg URLs are not detected.
469355	In a test environment with FortiTester, FortiWeb's proxyd crashes every minute when a request triggers a period block action in a CSRF or Start Page rule.
470600	The CLI command `diagnose debug disable` closes the debug output, but does not clear all debug settings.
470604	The HTTP RPS of 150 pservers is lower than six pservers when FortiWeb is in True Transparent Proxy mode.
471100	FortiWeb may not be able to communicate with a client when you specify an `ha-mgmt-interface-gateway`.
472509	After restarting FortiWeb AWS On Demand, the serial number may be lost.

Bug ID	Description
473947	FortiWeb does not check the SSL hardware status when there is an SSL error that causes the connection to close.
473966	Signatures may not correctly match on FortiWeb AWS.
476393	Proxyd may crash when FortiWeb performs CSS decoding.
476653	This bug applies only to FortiWeb 100D platforms: HTTPSD may crash when you attempt to log in from the web UI.
478009	If a client request uses the HTTP `CONNECT` method type, FortiWeb may hold the request and not send the request to the server.
478303	Proxyd may crash when FortiWeb can't connect to the OCSP server.
479650	When upgrading from 5.8.X, social security card detection may not work properly.

Known issues

This section lists known issues in version 5.9.0, but may not be a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
436376	If there is a hexadecimal code `%3d` in the parameter name or cookie name, attack logs may display the corresponding character = incorrectly.
468660	The following issue applies to only FortiWeb 2000E appliances: During autonegotiation, the LEDs for: • The management port and ports 1–4 are green at 100M and yellow at 1000M. • Ports 5–8 are yellow at 1000M. • Ports 9–10 are yellow at 10000M.
469093	This bug applies to only FortiWeb-VM on KVM: HTTPSD may crash when updating from version 5.8.5.
469369	This bug applies to only FortiWeb-VM on AWS: If you have a High Availability deployment with instances that use EC2-Classic, the failover time may take too long.
469371	This bug applies to only FortiWeb-VM on AWS: In a High Availability deployment, if a Host A (standby) and Host B (primary) switch so that Host A becomes the primary appliance, and later switch back, the elastic IP for Host A no longer binds. This is because FortiWeb doesn't support multiple elastic IPs to one interface address.
471903	In a signature rule, if the **Action** for the **Information Disclosure** option is set to `Alert & Erase`, the attack log message ID that FortiWeb generates in response to a rule violation will contain the erased information.
473184	When you delete a large number of rules, an error may occur if the requested URL's length exceeds the server's capacity limit.
475874	If FortiWeb loses the connection with FortiSandbox, sandboxd may crash due to an `out of memory` error.
478579	This bug applies to only FortiWeb-VM on XenServer: In a High Availability deployment, if the primary and standby appliances switch roles,

Bug ID	Description
	you can't access the pserver afterwards.
479855	In a High Availability deployment, FortiWeb cannot run a heartbeat on FortiGate VXLAN.